Securing Intellectual Capital: An Exploratory Study in Australian Universities

Journal:	*Journal of Intellectual Capital*
Manuscript ID	JIC-08-2019-0197.R1
Manuscript Type:	Research Paper
Keywords:	Intellectual capital, Data security, Knowledge management, Higher education, Universities
Abstract:	

Securing Intellectual Capital: An Exploratory Study in Australian Universities

Structured Abstract:

Purpose – To investigate the links between IC and the protection of data, information and knowledge in universities, as organizations with unique knowledge-related *foci* and challenges.

Design/methodology/approach – We gathered insights from existing IC-related research publications to delineate key foundational aspects of IC, identify and propose links to traditional information security that impact the protection of IC. We conducted interviews with key stakeholders in Australian universities in order to validate these links.

Findings – Our investigation revealed two kinds of embeddedness characterizing the organizational fabric of universities: (1) vertical and (2) horizontal, with an emphasis on the connection between these and IC-related knowledge protection within these institutions.

Research implications – There is a need to acknowledge the different roles played by actors within the university, and the relevance of information security to IC-related preservation.

Practical implications – Framing information security as an IC-related issue can help IT security managers communicate the need for knowledge security with executives in higher education, and secure funding to preserve and secure such IC-related knowledge, once its value is recognized.

Originality/value – This is one of the first studies to explore the connections between data and information security and the three core components of IC's knowledge security in the university context.

Keywords: Intellectual capital, Data security, Information security, Knowledge security, Cyber security, Higher education, University.

Paper type Research paper

1. Introduction

Intellectual Capital (IC) is the stock of knowledge held by an organization (Dierickx and Cool, 1989), and is made up of three components: human capital (HC) (the product of individual intellectual action, i.e. individual tacit knowledge), structural capital (SC) (organizational processes, systems and routines that structure intellectual assets into group property), and relational/customer capital (RC) (understanding of ex-firm intangibles) (Bontis, 1998). Knowledge is at the core of IC (Stewart, 1997; Renaud *et al.*, 2019) with organizations being considered "repositories and coordinators of intellect" (Quinn, 1992, p. 241), this being intrinsically linked to organizations' economic wealth and value creation (Paloma Sánchez and Elena, 2006). There is a growing interest (in both research and practice) into the role of IC in educational institutions (Bisogno *et al.*, 2018) and particularly in Higher Education (HE) (Paloma Sánchez *et al.*, 2009), where IC management is crucially important, given the knowledge-focused nature of their activities (Secundo *et al.*, 2015).

Reflecting this focus, a burgeoning stream of research has been dedicated to the study of IC components in universities. Five distinct *stages* of IC research have emerged (Bisogno *et al.*, 2018; Secundo *et al.*, 2018) but none of these is specifically linked to the preservation of IC, as impacted by the cyber era. Yet, as we will argue, universities are exposed to significant challenges in terms of securing their IC-related data, information and knowledge. Many universities have long histories, and existing structural assets, whose contribution to the value creation process is undeniably significant (Di Berardino and Corsi,

2018). Yet, it is important also to consider how universities *secure* their data, information and knowledge, given that their existing infrastructures are likely to pre-date cyber-attacks. We need to examine the ways in which universities traditionally transmit and disseminate knowledge, and consider how these practices are impacted by the security requirements of the cyber era. In this paper, we reveal connections between IC-related *knowledge security* and traditional *information security,* which is generally concerned with the preservation of data and information. The study of knowledge security (Desouza and Vanapalli, 2005), is relatively immature (Desouza, 2006; Renaud *et al.*, 2019), and, given the importance of IC within universities, we believe greater insights into this topic would be valuable to the HE sector as a whole.

Section 2 of this paper defines the IC concept and explores the related literature. We also consider extant methods of data and information security, i.e. the protection of the confidentiality, integrity and availability of data/information (the so-called CIA properties) (Von Solms and Van Niekerk, 2013) and links to *knowledge* security. We shall argue that the very nature of HE presents significant challenges when it comes to securing both data and information (Bongiovanni, 2019) and, inevitably, also organizational knowledge. Intrinsically, cyber security and HE seem subject to diametrically opposing pressures: on the one hand, there is the need to protect data, information and knowledge to preserve the three components of IC. On the other hand, there is a strong drive to share knowledge, to foster innovation and create international links and research collaborations across legislative boundaries.

Section 3 outlines our research framework and explains how we carried out our research. Section 4 presents our findings and Section 5 discusses them, and presents a

conceptualization of IC's links to information security within knowledge-intensive institutions such as universities. Specifically, we unpack IC's three foundational components and explain how these are influenced by extant data and information security practices in 10 Australian universities and one major research center. Section 6 concludes the paper and suggests directions for further research.

2. Review of the literature

2.1 Data, information and knowledge as constituents of Intellectual Capital

Researchers have conceptualized IC in different ways. Stewart (1997) aligns IC with knowledge, information, data and Intellectual Property. Nahapiet and Ghoshal (1998) describe IC as knowledge and knowing capability, whereas Dierickx & Cool (1989) refer to IC as "stock of knowledge". Asiaei and Jusoh (2015) mention IC's link to know-how and knowledge of manpower, databases, information technology, operating processes, customer relationships, brand, trust and cultures.

Researchers and practitioners alike have also identified ways to operationalize IC, to conceive it as a construct, with the purpose of measuring, assessing and preserving it. Bontis (1998) argues that IC is composed of three sub-categories of capital: human, structural, and customer/relational (HC, SC and RC). Human capital (human resources plus intellectual assets, Edvinsson and Sullivan, 1996) refers to the individual tacit knowledge possessed by the members of an organization, necessary for them to perform their functions and tasks. Structural (or organizational) capital refers to the structural tacit knowledge ingrained in the organization: mechanisms, structures, and cultures, which support individuals in their quest for superior intellectual performance. Customer (or relational) capital relates to the external dimension of organizations and is constituted by knowledge of marketing channels and customers. Central to the construct of IC are the concepts of data, information and

knowledge, these three existing in a specific structure. Data constitute raw facts and numbers which, once given meaning, become information. This, in turn, becomes knowledge when patterns are recognized within the information (Dretske, 1981). The importance of the relationship between the data-information-knowledge triad and IC has been stressed by Bontis (1998), who has described information as the raw product, knowledge as the finished product and IC as knowledge utilized to produce value. More recently, Tien (2013) maintained the hierarchical nature of the relationship and justified data analysis activities as an attempt to produce information from data; knowledge from information; and wisdom from knowledge. The emergence of innovative applications of modern technologies has led some authors to re-consider this relationship. For example, in the case of Big Data, information is conceived as structured data to be useful and relevant for a specific purpose. Subsequently, information, not data, prevails as the fundamental fuel of the Big Data society (De Mauro *et al.*, 2016).

Other authors conceptualize the data-information-knowledge structure differently. Drawing inspiration from the work of Tuomi (1999), Alavi and Leidner (2001) postulate a bidirectional connection between information and knowledge, whereby the former becomes the latter once processed in an individual's mind and *vice versa*: the latter becomes the former once codified. The authors contend that knowledge does not exist outside an individual's mind and can be conceived as a capability. As such, knowledge management is basically intended to create IC and information systems act in support of knowledge management by developing individual and organizational competencies and reinforcing the fragile knowledge sharing connections existing in organizations (Alavi and Leidner, 2001). At their core, knowledge management systems support the creation, storage & retrieval, transfer and application of knowledge (Schultze and Leidner, 2002).

In their literature review, Leal, Meirinhos, Loureiro, and Marques (2017) confirm the scarcity of research on cyber security management and IC, a view also shared by Trkman and Desouza (2012). In the latter paper, the researchers highlight the existing trade-off between knowledge sharing and knowledge risks and propose their version of the data-information-knowledge tripartite structure: data being the raw input to an interpretive process; information the aggregation of raw inputs plus application of processing techniques; and knowledge the collection of experiences, know-how, and 'gut feelings' that help employees make sense of information.

Among the first to do so, Bontis (1998) argues that organizations that securely protect their information possess high IC. La Torre, Dumay, and Rea (2018) revisit data, information, and knowledge processes and suggest that protection is needed across all components, for an organization to be able to defend its IC. This is demonstrated by the intrinsic relationship existing, for example, between privacy violations (individual level) and security incidents (organizational level) (La Torre *et al.*, 2018). The authors suggest a framework whereby data breaches impact on IC's traditional components: in particular, loss of confidentiality would affect HC, SC and RC; loss of integrity would affect HC and SC; and so would loss of availability. Questions around the potential impact that such losses of confidentiality, integrity and availability could have on all IC components remain. A more complete framework linking IC and information security is proposed by Renaud *et al.* (2019), who extend Von Solms and Von Solms' work (2018) and align IC protection with information, knowledge and cyber security efforts in organizations.

2.2 Technology adoption and Intellectual Capital in universities

As organizations tasked with innovating and producing research, universities epitomize institutions replete with intangible IC assets (Paloma Sánchez and Elena, 2006). In the

current wake of digitization, these institutions have a privileged position in exploring *technology affordances and constraints*, that is to say the potential for action offered by digital technologies, based on users' intentions (Nambisan *et al.*, 2017). The three main categories of university users are students, academics and professional staff. As protagonists of the HE experience, students epitomize the affordances of digital technologies in universities: these 'learners of the digital era' (Rapetti and Cantoni, 2010) seamlessly utilize the same technologies for both social and academic purposes. To name a few examples, *Whatsapp* therefore becomes a way to connect with friends, but also facilitates coordination of group assignments; the tablet is now the preferred note taking tool during lectures; and social networks are used to share various documents as well as to coordinate and socialize (Gallardo Echenique *et al.*, 2015).

Academic departments and laboratories abound with technology-driven experiments with PhD students and researchers exploring applications of a variety of technologies in different contexts. Digital artefacts (components, applications or media contents that offer a specific functionality to end-users), platforms (shared sets of services to host complementary offerings) and infrastructures (tools and systems for communication, collaboration and/or computing to enhance innovation) (Nambisan, 2017) are not only present in ICT-intensive departments (e.g., Computing Science and Engineering) but also in disciplines that were traditionally less attached to the usage of cutting-edge technologies (e.g., Social Sciences and Humanities). Examples of modern technology adoption trends by academics and professional staff members in universities include the exponential growth of HE institutions' presence on social media and the creation of dedicated contents for communication and marketing purposes (digital artefacts); the adoption of interactive, educational platforms to enhance the learning and teaching

experiences (digital platforms, e.g. Blackboard); and the diffusion of cloud computing technologies to support collaborative research projects (digital infrastructures).

Besides being at the heart of modern technology adoption trends, from a managerial perspective, universities face three specific challenges, namely (1) an increased demand for transparency on the use of funds, (2) a growing attention to social accountability as a result, among other, of greater autonomy, and (3) expanding competition resulting from reduced levels of funding (Secundo *et al.*, 2016).

In recent years, universities have seen a growth in their service portfolio beyond traditional teaching and research, in favor of the "third mission": the need for HE institutions to open up to the external environment, by transferring knowledge to stakeholders such as private and public organizations, civil society and larger public, with the ultimate goal of fostering economic and social growth of their regions and countries (Paoloni *et al.*, 2019; Mariani *et al.*, 2018; Secundo *et al.*, 2018; Etzkowitz *et al.*, 2000). In the light of these trends, activities such as inter-organizational collaboration, open innovation, research commercialization and public engagement are rapidly diffusing in universities. It is not surprising, therefore, that HE institutions have attracted a great deal of research on IC and knowledge management practices in general, topics traditionally attached to private organizations (Secundo *et al.*, 2015; Moustaghfir and Schiuma, 2013). IC approaches are increasingly utilized in universities as management tools, to measure, manage and report on the value of intangibles (Elena-Pérez *et al.*, 2011) , to the extent to which, according to the Observatory of European Universities, IC-related information should be compulsorily disclosed by universities (Sangiorgi and Siboni, 2017), a step perceived necessary to encourage efficiency, effectiveness and excellence in universities (Elena-Pérez *et al.*, 2011).

For the purposes of this research, an operationalization of the IC construct is required. The canonical, tripartite IC structure proposed by Bontis (1998) is the leading framework, with different nuances based on the individual studies. HC is varyingly defined as explicit and tacit knowledge of personnel (Ramírez *et al.*, 2007) or intangible value in people's competencies (Leitner *et al.*, 2014), and examples include the role of researchers and attracting the best professors and students (Secundo *et al.*, 2015). SC is defined as explicit knowledge associated with internal processes (Ramírez *et al.*, 2007) or intangible resources in the organization and examples include databases, intellectual property and research projects (Leitner *et al.*, 2014) or publication records of researchers (Secundo *et al.*, 2015). RC is defined as the spectrum of relationships developed by universities (Ramírez *et al.*, 2007) or intangible resources to generate value from internal and external relationships (Leitner *et al.*, 2014) and examples include networks with other universities (Secundo *et al.*, 2015).

One of the most compelling challenges for organizations is to encode the existence of individually-held knowledge and record this as an organizational asset. For this purpose, IC's main function is to organize knowledge resources in a manageable fashion, and this demonstrates the fundamental role of the human dimension of IC (Vagnoni and Oppi, 2015; Secundo *et al.*, 2016). Due to its completeness and granularity, the present research utilizes Ramirez, Tejada, and Manzaneque's operationalization of IC (2016) as the basis for its conceptual framework. Borrowing from prior work (Meritum Project, 2002; Hudson, 1993; Stewart, 1997; Mouritsen *et al.*, 2001), the three authors combine different nuances to produce the following definition of IC, which we complement with a fourth dimension, connectivity between components (Mariani *et al.*, 2018) (Table I).

Table I here

According to Low, Samkin, and Li (2015), universities mainly disclose information about HC and SC, and less about RC. In an Italian study, Sangiorgi and Siboni (2017) found that Italian HE institutions prefer to disclose IC that is related to the university as an institution (SC), rather than IC associated with their staff members (HC). Among the benefits of IC reporting by universities, Ramirez, Tejada and Manzaneque (2016) include using IC disclosure as a management tool to allocate resources, define institutional strategies, prioritize tasks, etc.; and as a medium for external communication, to attract resources in exchange for accountability. The concept of IC disclosure entails considerations on how well universities protect their stock of tangibles and intangibles: data, information and knowledge. To this end, the next section briefly illustrates information security issues in universities.

2.3 Insecure IC in Universities? Data, information and knowledge security in Higher Education

The literature reviewed up to this point emphasizes how threats to the data, information and knowledge collected, stored and managed in HE institutions have the potential to jeopardize their stock of IC. Based on the type of data, information and knowledge affected, this can happen at the HC, SC (organizational and technological) and RC levels.

Recent events have demonstrated how universities are seen as an increasingly more attractive target for cyber-criminals (Borgman, 2018; Chapman, 2019; Luker and Petersen, 2003). An investigation conducted by *The Times* in the UK revealed that hundreds of cyber-attacks have targeted top institutions including the Universities of Oxford and Warwick and University College London (Yeung and Bennett, 2017). In the United States, in January-July 2016, MIT was subject to more than 35 *Distributed Denial of Service* (DDoS) campaigns

(Mejia, 2016). These attacks affect data security and potentially compromise universities' SC (technological): by flooding targeted machines with random requests (data), they can compromise entire IT networks, effectively halting operations in universities. In so doing, DDoS attacks have the potential to affect HC (e.g., staff members' personal information) as well as RC.

Data security was also at the core of a recent, eminent cyber-attack perpetrated to the Australian National University: officials feared Chinese actors were behind the attack, in an attempt to recruit foreign students as informants, by acquiring their personal data (bank numbers, tax details, academic records and passport details) held by the university (McGowan, 2019). This case epitomizes a potential disruption of the university's HC and RC. Besides DDoS attacks or theft of personal identity details (e.g., social security numbers in the US, an instance in which HC is directly affected), there is also growing concern around the potential for sensitive information to be stolen from universities and sold to foreign states, in a cyber-warfare scenario (Yeung and Bennett, 2017). This event has the potential to impact a university's RC, by compromising established relationships with external stakeholders. As an example, knowledge security is jeopardized when external actors penetrate universities' IT networks in an attempt to 'steal' intellectual property to gain commercial advantages (Field, 2019). Universities feature a unique level of embeddedness for their end-users, which magnifies the potential vulnerability of the HC-SC connection in HE institutions.

Universities' open-platform architecture makes them particularly vulnerable to external attacks, due to the numerous access points they offer and the extensive amount of data and information they hold at any given time (SC) (Liu *et al.*, 2017). Once in a university

network, attackers can access the personal data of academics, students and professional staff (HC). With the expansion of activities in which universities are involved (third mission), the types of managed data increase, and the security of such data has become increasingly complex. As data stewards, universities must implement adequate governance mechanisms which are, at best, nascent in the university environment (Borgman, 2018). Furthermore, research also shows that diffusion of an adequate information security culture is still incomplete in universities (Hina and Dominic, 2016).

Culturally speaking, the HE environment is characterized by a sense of intellectual freedom (Martin-Sardesai and Guthrie, 2018), which stimulates experimentation and open scholarly enquiry and pushes its actors towards information sharing, inter-organizational collaboration, international outreach and individual autonomy (Luker and Petersen, 2003). Security issues deriving from a university's cultural stance have the potential to affect its SC (in particular, its organizational capital). A study on information security policies in HE has highlighted that *personal usage of information* and *Internet access* ranked tenth (second-last) and eleventh (last) in a ranking on the topics mostly covered in information security policies implemented by universities worldwide (Doherty *et al.*, 2009). The same two topics ranked significantly higher (respectively third and second) in a similar ranking in other industries, indicating the different relevance that these topics have.

IC is not the only form of capital to consider when examining the security of data, information and knowledge in universities. The costs associated with implementing information security are another issue that IT managers face in modern universities, where pressure on cost containment is often dominant (Collini, 2017). As a result, universities

frequently embrace the *"*least cost and least resistance*"* (Lane, 2007, p. 238) approach to information security, which can negatively impact their security performance.

3. Research framework

Our approach stems from the *interpretive discourse* in studying knowledge management practices (Schultze and Leidner, 2002). Stenmark (2000) argues that in the interpretive discourse, technology can be utilized to formalize tacit knowledge in organizations where collective action emerges in systems of distributed knowledge. The focus of investigations in interpretive studies is on information systems research. Based on this approach, our study adopted the research methods described in the next section.

Our research investigates the constituents of IC in universities, with a focus on how HE institutions can protect their HC, SC and RC. We adopt Ramirez, Tejada and Manzaneque's (2016) tripartite structure of IC and posit that HC has a predominant role in universities and a bi-directional relationship with RC (Secundo *et al.*, 2016), and that SC, as instantiated in organizational and technological capital, has a support function (Vagnoni and Oppi, 2015; Bontis, 1998). To further operationalize our framework, we utilize Tien's (2013) data-information-knowledge framing (see also Trkman and Desouza, 2012), in its non-hierarchical version (Alavi and Leidner, 2001; Tuomi, 1999). In the present research, data, information and knowledge are considered as *building blocks*, instantiations of HC, SC and RC, whose security is essential to IC protection (Figure 1).

Figure 1 here

For example, consider a researcher at University A collaborating to carry out a study with a researcher at University B. They first collect data about the people they are studying,

which has to be secured, yet shared between the researchers (this is where SC becomes relevant). Such data can be secured using traditional information security techniques. As the researchers analyze their data, it becomes information, which also needs to be shared securely between the SC components of both universities. As the researchers work together, their personal relationship matures and becomes part of the RC of both universities. Next they collaborate and write a research paper together. Both now have knowledge that has grown from the information their study generated. The knowledge is part of the HC component of IC. Some is encoded within research publications, but much of the new knowledge will remain tacit and ephemeral: held within the two human actors' minds.

3.1. Research design and methods

This study focused on unpacking issues associated with data, information and knowledge security, as perceived and represented by senior officials in Australian universities. The sample was specifically selected to involve individuals who held both strategic and operational roles. Over a period of months, commitment was obtained from individuals holding relevant posts within universities, via the network that represents them at a State level.

Being focused on specific senior members with particular organizational responsibilities, the sample selection was partly purposive (Jupp, 2006) and convenience-based (Bryman and Bell, 2015). The final sample of participants consisted of nine senior officers (predominantly IT Directors, CIOs, and Cyber security Managers) from research-active, public, teaching universities, one from a private university and one holding an equivalent position in a public agency undertaking scientific research. Involved institutions were spread across three states

in Australia. Australia has 43 universities which are multi-disciplinary, self-governing, under federal or state and territory legislation, and granted responsibility for their own management. In recent years, Australian public universities have been pushed to adopt a corporate managerial approach (Christopher, 2014), characterized by efficient use of resources, enhanced institutional management, policy and planning, and increased number of stakeholders to satisfy (Martin-Sardesai and Guthrie, 2018).

Stemming from an *interpretivist* approach (Patton, 2002), this research assumes that social reality is created by the interaction of social actors and researchers' main task is to make sense of the collected data through interpretation, to gain understanding. Consistent with an interpretive discourse approach (Schultze and Leidner, 2002), our study is qualitative. The format of engagement was therefore designed around a semi-structured interview question set. Interview questions were formulated in an attempt to balance research requirements with knowledge and background of the interviewees (see Appendix 1). None of the interviewees had experience with IC, but all had significant expertise in data, information and knowledge security, as either specialists in cyber security (e.g., security managers) or IT executives (e.g., IT Directors and CIOs). Interview questions mainly referred to data, information and knowledge security issues affecting HE institutions, with a view to unpacking their impact on the whole organization. To validate the questions, feedback on the research design was provided by the board of the network of universities' IT Directors in one Australian State. Both the participant and the board confirmed clarity, pertinence and relevance of the research design and questions. The interviews took from 30 to 75 minutes and were recorded, with permission, and later fully transcribed to support content analysis by members of the research team. The research design was subject to institutional ethics approval.

3.2. Analysis

Interview analysis was conducted using *abductive reasoning* (Timmermans and Tavory, 2012), whereby rigorous methodological analysis was used to explore interviewees' personal, social and intellectual positions in relation to the topic. As such, rather than seeking confirmation of *a priori* categories of data, information and security risks derived from extant literature, the focus was on, *"breaking down, examining, comparing, conceptualising and categorising data"* (Corbin and Strauss, 2015) such that emergent classes of cyber security factors might be postulated, *"by making connections between categories"* derived of individual experience. Content analysis of the transcribed interviews was conducted in two stages. The first involved *close reading* of the material to identify critical issues highlighted by participants and to group these under common categories. The identified categories were then abstracted to relate them to a smaller number of more general, conceptual classes (Miles and Huberman, 1984), using an iterative process of comparison and testing (Spiggle, 1994). In order to avoid interpretive bias, two researchers independently coded the collected data and then compared and contrasted their coding, to identify discrepancies and gaps (Marshall and Rossman, 2011). The researchers then discussed cases of misaligned coding to find an agreement on the nature of the information portrayed by the excerpts under analysis before comparison and collation into a single report. To validate the findings, a synthetic presentation was submitted to the participants to collect feedback on missing elements and interpretation errors.

The results of the analysis are outlined and discussed in the following section, in which we link participants' understandings of data and information security risks to extant literature and theory on IC and its components.

4. Findings

The 11 interviewees agreed that data, information and knowledge security represent a challenge, as demonstrated by the following excerpt:

> *"You will never going to be on the front foot from a cyber-perspective…the only thing that will give you absolute security and control is disconnecting from the Internet and you put your technology in Fort Knox."* (Resp. 1)

This excerpt also sets the tone for considering technology as an SC element (in particular as a technological capital component). The following sub-section exemplifies data, information and knowledge security issues associated with the individual dimension of IC, HC.

5.1 Human Capital

Data revealed several security threats in universities related to the experience, perceptions and skills of individuals. Most interviewees agreed on the challenge constituted by *spear phishing* (e.g., interviewee 10) and, in general, *social engineering* (*"almost on a weekly basis"*, as indicated by interviewee 2) as sophisticated ways of exploiting individuals' propensity to fall for enticing messages (e.g., emails and messages on social media), for the purpose of extorting personal information (e.g., credit card details). In universities, spear phishing targets all stakeholders, including students, academics and professional staff, and its effectiveness is influenced by the ability of such individuals to recognize it and act accordingly (for example, reporting a suspicious email to the IT department). Spear phishing and social engineering rely on information attackers gather about their victims to perpetrate targeted attacks. They therefore represent instances of information security impacting HC.

In order to gauge the effect that the individual approach to security has on the overall stock of IC in the university, one of the interview questions required participants to

elaborate on the nature of data and information security, identifying them as being intrinsically more human or more technical. Interviewees' answers had a two-fold focus: on the one hand, participants elaborated on organizational vulnerability to cyber-threats, an aspect stemming from a SC perspective (organizational capital). However, despite acknowledging the relevance of the technological components (e.g., effectiveness of malwares and structural weaknesses of security architectures), interviewees mainly agreed on its predominantly human-related nature (e.g., *"…humans are the problem"*, interviewee 10). In particular, the topic of end-point vulnerability was extensively discussed:

> *"The consequences of not following good cyber-security practices are probably not well understood."* (Resp. 9)

> *"With the amount of spear-phishing attacks we had in the last six months…we had all the technology sorted, but the way they got in, it's the human clicking…"* (Resp. 5)

The findings presented so far mainly refer to unintentional behaviors by individuals. Several participants also discussed instances in which researchers who operate in research-specific environments that require stability and control, oppose structural security practices, such as *software patching,* which could compromise the integrity of their data (SC, technological capital). In the case of PhD students, research usually lasts three years and more, and a lack of updates over such an extensive timeframe could pose serious security consequences. This tension was represented as follows:

> *"We regularly get pushed back by researchers saying: 'Your controls are too tight; we can't run software or do the experimentation we want to do.'"* (Resp. 1)

HC includes consideration of the motivation to act (or not to act) in given ways by individuals operating in organizations. Among the most common difficulties that the IT security team encounters is the complacent attitude of some employees, who do not value data and information security and perceive it as a distraction from their *core business*. In association with instances of SC (e.g., in its organizational form, organizational culture), a change in the security attitude of the university was described by most interviewees as a slow process. One of the problematic aspects was the disconnect between individuals and information security, as represented in the following passage:

> *"The message should be that cyber security is about enabling digital transformation to occur. In this way, cyber security would become more meaningful to [people]…but now [cyber security] is portrayed as cyber-terrorism…and people disconnect from this."* (Resp. 2)

Nonetheless, several interviewees acknowledged that their organizations were changing towards a view of cyber security, not as a liability, but as a source of competitive advantage. This translated into significant differences across universities in terms of staff members dedicated to information security (*"…some universities may have 3-4 people. I've got 15 and a multi-million dollar budget"*; interviewee 7). This HC element contributes to the university's SC.

Specific analysis was needed for *insider threats,* another highly debated topic, reflective of a noteworthy debate in many industries. Interviewees mentioned that this threat could possibly take two forms: as the result of malicious behaviors by individuals; or as unintentional acts committed by employees. Data revealed that the latter is most prevalent:

"Insiders are not necessarily working for a criminal organization […] it's actually more internal people making poor cyber security judgement." (Resp. 6)

Based on their origin, insider threats can be considered reflective of sub-optimal HC (for example, resulting from poor knowledge of information security or insufficient motivation to behave securely) or from adverse effects of RC (for example, when an employee unwittingly acts upon direction of external, criminal organizations intending to target a specific university). Findings ascribed to the field of HC demonstrate close connections with SC, the topic of the next section.

5.2 Structural Capital

In general terms, several interviewees agreed that the *attack surface* of universities is expanding *("…organizations are increasing their cyber security footprint…"*; interviewee 2). This is due to an increasingly multi-modal environment, which significantly spreads data distribution (e.g., BYOD; interviewee 9) and raises further challenges in terms of balancing individuals' use of personal devices (HC) with corporate systems (SC). In association with a university's RC, progressively longer supply chains and flexible outsourcing arrangements seem to push the center of gravity of security controls away from the university premises. In this scenario, it becomes more difficult for IT security teams to identify and monitor potential *back doors* (interviewee 1), as these may fall outside organizational boundaries.

In contrast, several interviewees acknowledged the greater flexibility that solutions like cloud computing (technological capital) provide, enabling employees to work remotely, in a variety of locations, together with maintaining the integrity and reliability of their data and information. Cloud computing was also described as generally efficient, with the potential to alleviate the financial burden on capital expenditure (*CAPEX*) and shift it to

operating expenditure (*OPEX*). This last point, in the interviewees' words, makes investment in cloud computing (as opposed, for example, to on-premises data centers) more appealing from a business perspective.

Several interviewees acknowledged the diffusion of IoT in universities. While recognizing the benefits of real-time data collection deriving from this SC component (technological capital), participants also indicated that its misuse could potentially lead to serious breaches (for example, more effective *Distributed-Denial-of-Service attacks, DDoS*; e.g., interviewees 3, 5, and 10), especially considering that universities host an extensive amount of *always connected* devices (e.g., sensors in medical laboratories and robots, but also more traditional devices such as printers, CCTV, etc.). An aspect of IoT that was indicated as particularly concerning for universities, was the increasing exposure deriving from the growing interconnection between the physical and the digital world (*"…the convergence between the information technology and the operating technology"*; interviewee 2) that IoT enables.

> *"IoT is a growing concern: it captures larger amounts of data, imagine for example for research purposes, but there will always be ways to exploit such data."* (Resp. 3)

Concerns around IoT epitomized an underlying issue mentioned by numerous interviewees, the juxtaposition of present-day IT capabilities with legacy-systems that are still largely present in modern universities (a technological capital issue, SC). One participant illustrated the *contagion effect* intrinsic to having a previously physical-only, standalone device, for which data and information security was not activated by default, transformed into a gateway for a larger digital network (interviewee 5). On the same topic, interviewee 3 explained that architectures with default security can be more easily developed utilizing

green-field components, as opposed to legacy ones. In this interviewee's words, the latter can only have *"tagged-on"* (and not default) security.

Besides the role of technology in protecting (or jeopardizing) the security of data, information and knowledge in universities, participants elaborated on another component of SC, namely organizational practices and structures aimed at preserving the confidentiality, integrity, and availability of information (organizational capital). These arguments often revolved around the consideration of whether information security could be considered an operational or a strategic activity performed by universities. Consistent with current debates in other industries, interviewees agreed that a "strategic turn" is indeed necessary for information security to receive the necessary consideration in universities. In the interviewees' words, one of the most powerful leverages to ease this transition is raising awareness around the destructive impact of security breaches.

In close connection with RC, reputational risks are generally perceived as particularly significant for universities, especially with the current, expanding student bases. Interviewees explained that the reputational aspect of data and information security is particularly debated in the board of directors' meetings (SC, organizational capital). Such conversations refer to the essence itself of HE institutions as organizations tasked with diffusing knowledge (as well as protecting it). Consequently, their value is eminently strategic (knowledge security issue affecting SC).

However, most participants believed that data and information security are still seen as an operational, rather than a strategic issue, in the sense of conducive of shifts in the competitive balance. Because of this, interviewees concluded that data and information

security is perceived as a risk management issue, for which mitigation attracts the most effort in terms of SC.

> *"I think for an organization such as ours, [information security] is still a risk management issue, I think it will drive eventually towards strategic, but it's something that is a cultural change and I think it takes time."* (Resp. 5)

This scenario could mutate if a major security incident happened, which would likely push a change in mindset, as witnessed by interviewee 3. However, with a lack of practical examples on the implications that a security breach could have, interviewees explained that justifying information security expenditure is a challenging task, especially when the board of directors and the IT security team speak different languages, with the former more business-minded and the latter more technically-oriented.

> *"As an IT manager, how do you communicate with company directors in non-technical ways, as they usually do not come from an IT background?" (Resp. 3)*

Generally, interviewees agreed that return on investment on information security is difficult to demonstrate and several of them argued that their board of directors might prefer to take some limited risks, rather than over-investing in information security. One of the arguments to justify this stance was that growth is enabled by taking acceptable levels of risk, especially in the university sector, naturally prone to technology adoption and innovation. In the same direction, data and information security, as with any other risk management investment, may require significant investment and not deliver quantifiable results, other than avoiding major losses.

> *"The boards of directors are looking at growth, and there is no growth without risk…and sometimes they might go: 'Is IT crying wolf yet again?'… It's a very fine line."* (Resp. 1)

Concerns were also raised about the potentially cyclical pattern of information security investments, whereby the current hype around cyber security could wane when other priorities emerge:

> *"Maybe in two years' time someone may be: 'Well, security had enough money in the last years, now it's time to invest in something else.'"* (Resp. 11)

5.3 Relational Capital

The complex relationships that universities have with service providers emerged in our interviews, especially in the field of data and information security. Service level agreements allow IT departments to ensure some level of control over vendors' activities, at least in terms of business continuity management in case of a breach of contractual terms. Contract management was therefore considered a crucial component of data and information security, to the point that one participant argued that one of the main duties of the IT department is managing vendors (RC), and not IT itself (interviewee 5).

Interviewees also indicated that one way to ensure enhanced control is to only engage with vendors based in Australia, in order to keep data onshore and ensure compliance with Australian legislation. The interviews, however, showed that effective contract management is a challenge, mainly due to the difficulty in assessing vendors' security performance. One interviewee argued that they would love to be able to completely outsource their information security function, should they identify a vendor capable of assuring outstanding security at a reasonable price (interviewee 3). Finally, on a

higher level of abstraction, when discussing contract management, several interviewees elaborated on an essential component of RC, trust, and the role it has in managing contracts with third-parties:

> *"In cloud services, trust is earned."* (Resp. 5)

> *"[Third-party] contracts are a proxy for trust, but they're not a perfect one."* (Resp. 3)

Regardless of the level of trust embedded in the delivery of security services, interviewees expressed concerns around the erosion of control (and security) that apparently comes with technological solutions such as cloud applications (technological capital that impacts RC), as witnessed in the following excerpt:

> *"Cloud computing is a reality of life, and it's a two-edged sword as it offers benefits…But you also lose some controls…when the updates are being done? How do you manage your data…how do you know how secure [the vendor] is?"* (Resp. 3)

Interviewees also discussed the implications of the current push for internationalization in HE. The increase in international travel requires consideration of the security repercussions of their carrying and utilizing university-owned devices on these trips. One mentioned an instance where researchers accessed public Wi-Fi networks in foreign countries where cyber security regulations were less stringent (interviewee 4).

5.4 Other data, information and knowledge security issues

The interconnected nature of IC's components was confirmed, in the form of topics whose nature cuts across HC, SC and RC. Several interviewees discussed the importance of data and information security awareness in universities and described it as an organizational reaction (SC, organizational capital) to phenomena that are eminently individual (HC).

Interviewees said that, at the end-point level, the university environment exhibits its diversity, with several categories of users coming from different cultural backgrounds and having different views on data and information security (e.g., *"…we manage over 100,000 identities"*; interviewee 7). From the interviews, it became clear that this complexity renders a standardized, one-size-fits-all approach to end-point security only partially effective. Consequently, interviewees stressed the importance of working on the individual information security awareness (HC) to enhance the security culture of all users (SC, organizational capital). Interviewees mentioned different practices used in their universities to raise information security awareness. All, however, agreed that such practices need to be complementary, and the best way to increase awareness is by providing a mixture of methods:

> *"We try to keep [information security] front of mind, it's a deliberate campaign, but it's not just posters splashed around the walls, it's more a mindset of a culture about whatever we do, it needs to be safe."* (Resp. 4)

Interviewee 9 explained that in their organization, a first approach to information security awareness is the launching of internal campaigns, organizing of events, and conducting information security training in general (SC, organizational capital). A second phase requires one-on-one contact with the university players, for the IT security managers to account for the diversity of their *customers* (e.g., academics and students) and customize information security awareness to their needs and capabilities (interaction between SC and HC). However, the generally scarce resources dedicated to information security render this exercise hardly sustainable, considering the high number of individuals to approach. As a result, as mentioned by one interviewee, often external media reports on eminent cyber-

breaches (potentially impacted by the stock of RC a university holds) have a higher impact on employees than internal training practices.

Considerations were made by interviewees on the availability of knowledge held by internal and external actors, with current trends potentially posing relevant challenges for the "defenders". In general, participants noted that malicious tools on the *dark web* (in particular, re-purposed government surveillance tools) are relatively easy to access and use, which increases the number of potential attackers and gives them a competitive edge over IT security managers (interviewee 3).

> *"Anyone can be a hacker. Kids coming out of school have much more IT knowledge than people that just graduated a couple of years ago."* (Resp. 4)

External factors did not only refer to the malicious intentions of attackers, but also to the surrounding social, economic and legal environment and how this has the potential to impact IC in universities. One of the interview questions asked interviewees to elaborate on the impact that legislation (such as the *Notifiable Data Breaches scheme*, which obliges organizations affected by data and information security breaches to disclose them: www.oiac.gov.au/privacy/notifiable-data-breaches) would have on data and information security. Opinions on this matter were generally aligned around the positive impact that such legislation would have on raising awareness on security, by impacting the knowledge of information security held by individuals (HC).

5. Discussion

Our investigation confirmed the challenge of securing data, information and knowledge within universities. From an IC perspective, universities are characterized by the prominence of HC, whereby knowledge residing with individuals is influenced by their role within the

organization and by their backgrounds (e.g., prior experience and culture). Given the variety of profiles existing in universities, ranging from specific roles (e.g., academics, professional staff, students, other stakeholders) to cultural differences (e.g., the push to internationalization, which has broadened the spectrum of cultures operating in HE), HC takes numerous forms, and its assessment has to account for such variety.

An interesting finding of our research relates to the impact that sub-optimal knowledge at the individual level has on the security of data and information in universities. Participants in our interviews emphasized the fact that end-users in universities have very different understanding of information security practices. Behaviors that, for some, may be legitimate (e.g., sharing data on non-accredited cloud platforms), are, to others, a clear violation of corporate security policies. Therefore, individual knowledge *qualitatively* impacts the overall amount of HC (and, by implication, IC) in a university, which suggests that assessing HC requires reflecting on the adequacy/non-adequacy of individual tacit knowledge in an organization, not just its binary presence/absence. This finding is consistent with literature stressing the importance of calculating HC loss (besides acquisition) in HE institutions (Martin-Sardesai and Guthrie, 2018).

On this note, a first conceptual bridge between HC and SC is revealed by our research. IT managers highlighted the importance of information security training in establishing (and then elevating) shared security awareness, a *level playing field* among end-users in universities: such training, as codified knowledge existing in an organization (SC) is used to influence and improve tacit knowledge held at the individual level (HC). *Vice versa*, the quality of individual knowledge serves as a *scale* to weight and customize security

training programs and courses. This suggests that HC and SC have a symbiotic relationship in universities.

The present research postulated that data and information, together with knowledge, constitute instantiations of HC. The results of our analysis demonstrate that, by virtue of a diffused *ethos* of academic freedom and the multi-modal nature of universities (Borgman, 2018; Martin-Sardesai and Guthrie, 2018), individuals enjoy a significant level of control over the data and information they collect and store and the knowledge they produce in HE institutions. Compared to other public and private organizations, the boundaries between individual and organizational intellectual property are fuzzier, to the point in which HC created in one university in the form of data or information (e.g., a research project), could be translated into knowledge in another university (e.g., when the investigator moves to another university). Similarly, the resulting knowledge could be formalized as SC in a third university (e.g., when the investigator moves to another university and publishes a paper based on previously conducted research). These dynamics highlight, once again, the challenges related to HC and SC protection in HE.

Defined as *"knowledge that stays within the firm at the end of the working day"* (Meritum Project, 2002, p. 11), SC represents the purest organizational form of knowledge present in a university. Due to their roles, our interviewees mainly elaborated on two elements of SC: technology and organizational practices to secure data, information and knowledge. Our findings highlight the need for a combination of the two. In particular, the need to complement traditional, technical defenses (e.g., IT security architecture) with organizational, human-focused interventions (e.g., awareness campaigns) is widely recognized in universities, and so is skepticism for a centralized, *one-size-fits-all* solution.

This is consistent with recommendations in the literature that HE institutions should avoid centralized information security models typical of corporate IT departments in favor of *"embraced autonomy"* (Adler, 2006, p. 58), a model that aligns universities' asymmetric structure with active participation and engagement in the information security efforts by their constituents (e.g., campuses, branches, colleges, departments, etc.). Conceptually, investing in technology and advisable security practices translates into SC investments. Our research suggests that senior IT managers utilize this framing as a promising perspective for conversations around information security budgeting with university management, perhaps more receptive to a business-based approach to security.

The existing literature argues for a supporting role of SC, which facilitates the development of HC and RC (Vagnoni and Oppi, 2015; Bontis, 1998). Data collected in this research seem to align with this: interviewees extensively discussed the functional role of technology and organizational practices in promoting organizational activities and in building a solid network of external stakeholders. Similar to HC, SC is instantiated through data, information and knowledge at the organizational level: for example, a research dataset owned by a university department; a scientific report elaborated from such dataset; and the associated expertise residing within a research team. Again, assessing SC entails evaluating the quality (and not just the quantity or size) of the data, information and knowledge produced at the SC level. Interestingly, however, negative events affecting SC and its instantiations seem to have the potential for greater adverse effects than similar events affecting HC: an example is the case in which an ill-designed information security policy is disseminated through training throughout the university, or a malicious external agent (e.g., a hacker) has access to a database of login credentials. This further corroborates the view of SC as an essential supportive component.

Universities' roles as innovation hubs within an ecosystem of public and private organizations, civil society and other constituencies pertains to their RC, a topic only recently discussed in the field of HE (Paoloni *et al.*, 2019). The emergence of universities' third mission (Etzkowitz *et al.*, 2000) has brought increased focus on how to secure the portion of IC deriving from connections with the other institutions. Several interviewees demonstrated heightened awareness of issues associated with the protection of intellectual property. Similar to HC and SC, this element entails the need to strengthen RC in universities, and not merely to report on its presence/absence in a binary fashion. The acknowledgement of an increased role for universities in national and international ecosystems comes with the growing importance that reputation, as one of the foundations of trust, has for such institutions. In this sense, a breach in the data, information and knowledge security systems of universities can trigger significant negative consequences such as lost trust, reputational damage and impaired RC. Unlike La Torre, Dumay and Rea (2018), we argue that regardless of data breaches' nature (as loss of confidentiality, integrity or availability of information), impacts on RC through reputational damage are always possible and always significant.

Our study unpacked the relationships between the three IC components and their substantiations: data, information, and knowledge, from an information security perspective. Unsurprisingly, given the intangible nature of knowledge, considerations around the latter emerged to a lesser extent from the participants' interviews. The majority of the collected data were coded around data and information security. As for the tripartite structure of IC, the spread of data was more consistent, with HC attracting slightly more statements. We synthesize our findings in Table II, to exemplify instances of data, information and knowledge security within HC, SC and RC, in the form of interview excerpts,

emerging themes and hypothetical, real-world examples outside the collected data. We have provided the latter to fill 'gaps' that participants' statements did not address.

Table II here

Our investigation emphasized how the very organizational boundaries of universities appear vaguer, as compared to other public and private organizations. Based on our data, we have identified two types of "embeddedness" that characterize the organizational fabric of universities. *Vertical embeddedness* refers to the integration that different categories of end-users (mainly students, academics, professional staff and stakeholders "sitting on the fence") have within a university. Vertical embeddedness manifests at both the HC and SC levels. In terms of HC, universities have different categories of end-users; traditional provider-costumer roles are ill-defined, and students are arguably at the same time *clients* (they pay fees) and *providers* (they produce knowledge, HC that becomes formalized as SC).

Moreover, individuals have different levels of understanding and perceptions of data and information security. In terms of SC, they all have access to basic shared facilities and technologies and all should act upon established security policies and practices. The dynamics associated with vertical embeddedness originate at the HC level but, given the configuration of universities, have the potential for adverse events such as data and information security breaches at the SC level. To tackle this, the different degrees of understanding of information security (HC) would require a customized approach to information security management (e.g., training, SC). Yet, this usually does not happen in universities; training is administered using a *blanket* approach that does not feasibly account for stakeholder nuances. *Horizontal embeddedness* refers to the inter-

organizational integration that exists across HE institutions and other public and private organizations, in the light of increasing international collaboration and third mission activities. Horizontal embeddedness manifests at both the RC and SC levels. In terms of RC, universities promote practices such as students being involved in international exchange programs; academics sharing and publishing anonymized datasets and co-producing research across countries, or being invited as *visiting academics* to different institutions; and non-academic staff members working on strategic partnerships around topics such as accreditation or education delivery (e.g., *Massive Open Online Courses, MOOCs*). In terms of SC, these practices are accompanied by supportive efforts, and investments, such as the award of joint degrees, the creation of shared IT networks (for example, *Eduroam*: www.eduroam.org), the constitution of grants aimed at promoting international collaboration, the promotion of knowledge exchange with public and private companies, etc. The dynamics of horizontal embeddedness originate at the RC level, but have the potential for data and information security breaches to manifest at the SC. Figure 2 represents the relationships among vertical and horizontal embeddedness and the components of IC.

Figure 2 here

In summary, vertical embeddedness in universities has the potential to enrich these organizations' stock of HC, by increasing the number and variety of tacit and explicit "knowledge nodes" in the network (e.g., knowledge created in a project where an academic's expertise is combined with a student's propensity to innovate, as supported by a competent professional staff members who suggest funding opportunities). This can in turn

increase SC (e.g., organizational capital such as research outputs) and RC (e.g., impactful research attractive to external players). On the other hand, the diffusion of nodes in the university network increases the university's digital footprint and presents data and security issues, with the potential, through the *contagion effect*, to disrupt SC (technological, but also organizational capital) and in turn RC (e.g., loss of reputation). The same applies to horizontal embeddedness, whereby close connections with external stakeholders multiply value-creation opportunities (e.g., knowledge transfer), increasing the stock of SC (e.g., practitioners' seminars guided by academics) and HC (e.g., academics benefit from real-world exposure). At the same time, horizontal embeddedness creates opportunities for security issues to emerge as a result of shared IT networks and infrastructures. Contagion could ensue, and so could disruption of SC and, in, turn HC.

5.1 Research implications

The conceptual framework we utilized is based on the tripartite IC structure proposed by Ramirez, Tejada, and Manzaneque (2016). The framework was reliably mirrored in the data offered by the participants, in particular in the division of SC in technological and organizational capital.

The implications of our findings are*, first*, that the roles played by the actors in universities have the potential to impact the quality of HC held by the university at any given moment. We therefore recommend that future studies on HC in HE account for the typical university profiles (students, academics, professional staff and other stakeholders) and their specificity *vis-a-vis* the contribution to HC (vertical embeddedness).

Second, the specific characteristics of organizations and other constituencies interacting with universities have the potential to influence the quality of RC. Profiling such characteristics in a discrete taxonomy (horizontal embeddedness) is a much more complex task than for HC, and we recommend that, at least, future studies assessing RC in HE consider the relationships between a university and its external partners based on the nature of the involved activities: teaching, research, service, and third mission.

Third, we suggest that future studies aimed at assessing SC in universities account for the role and influence of HC and RC. Our research also demonstrated that framing data, information, and knowledge as substantiations of IC's components is a promising approach.

We have 'problematized' these concepts by exploring the associated security issues, a currently 'hot' topic in HE. The information security literature has concluded that data breaches are not just a technical issue to be dealt with by IT departments (von Solms and

von Solms, 2004). The acknowledgment of the human and organizational side of information security has been accompanied by significant calls for researchers to further unpack the human and managerial determinants of data breaches (Siponen *et al.*, 2014; Soomro *et al.*, 2016). An IC approach shows promise, in particular if preceded by a solid exploration of the extent to which data, information and knowledge (as either a hierarchical trio or a homogeneous group) contribute to the different components of IC.

From a practical perspective, our study demonstrates that IC protection is not possible without data, information and knowledge security. As knowledge-intensive organizations, if universities want to maintain their competitive edge, they need to improve the ways in which they protect their data, information and knowledge, both tacit and codified. At the same time, as mentioned by several interviewees, HE's proneness to embrace technology adoption and innovation (Nambisan *et al.*, 2017; Nambisan, 2017) requires these institutions to balance security (as controls and barriers, but also as culture) with openness, a dichotomy demonstrated by the horizontal/vertical embeddedness levels proposed in this investigation.

Ultimately, this research provides senior IT security managers with an original framework to illustrate the potential adverse effects that poor data, information and knowledge security may have on universities' IC, as declined in its three components. Such framework can be fruitfully utilized to substantiate these concepts before executive members in universities, who do not necessarily have solid knowledge in information security management.

5.2 Limitations

Similar to any other, research, our study has limitations.

First, the adopted key informant methodology has the potential to suffer from potential biases (Kumar *et al.*, 1993). We interviewed senior IT managers and executives, who have predominantly contributed in the fields of SC and HC. However, their function is embedded in the component of IC around which HC and RC pivot. Their selection was considered an efficient way to gather meaningful information, conducive of a holistic view on IC. Yet it must be acknowledged that our sample represents around 25% of the population of Australian universities from three (out of 7) States and Territories in the country.

Second, our findings should be confirmed by means of a quantitative investigation. A large-scale survey designed around the results of the present paper is a possible avenue.

Third, our results represent the Australian case. Given the impact of country-specific factors (e.g., legislation, governance in HE, funding models, etc.), similar studies should be carried out in other countries, in particular to explore the usage of IC as a reporting and management tool (Elena-Pérez *et al.*, 2011), but also as a tool for external communication (Sangiorgi and Siboni, 2017; Ramirez *et al.*, 2016), a topic that usually attracts significant attention in information security management.

6. Conclusions and Future Research

This research demonstrates a degree of complexity of IC security in HE institutions that goes beyond the tripartite structure of IC. We unpacked the elements of HC, SC and RC, confirming, as argued in the literature (Vagnoni and Oppi, 2015; Mariani *et al.*, 2018), the importance of the relationships between such components (connectivity) as a fourth element. Our research explored the connection existing between IC and its various instantiations in universities' data, information and knowledge, highlighting the crucial

nature of information security structures and measures in protecting the organization's IC and ensuring that they can benefit from this crucial asset.

Future research is recommended to replicate the study in other countries, to control for possible factors associated with state legislation. To this end, we have plans to conduct a similar study in universities and research centers in the UK and US. We also plan to explore the exact relationships between the concepts of data, information and knowledge; the collected data could not provide a definite answer to the question whether a hierarchical order exists or whether some other, more complex relationships better describe how these concepts interact.

Funding

This research was not funded by any specific grants in the public, commercial, or not-for-profit sectors.

References

Adler, M. P. (2006) "A Unified Approach to Information Security Compliance", *Educause Review,* 41(5), 46.

Alavi, M. and Leidner, D. E. (2001) "Knowledge management and knowledge management systems: Conceptual foundations and research issues", *MIS Quarterly*, 107-136.

Asiaei, K. and Jusoh, R. (2015) "A multidimensional view of intellectual capital: the impact on organizational performance", *Management Decision,* 53(3), 668-697.

Bisogno, M., Dumay, J., Manes Rossi, F. and Tartaglia Polcini, P. (2018) "Identifying future directions for IC research in education: a literature review", *Journal of Intellectual Capital,* 19(1), 10-33.

Bongiovanni, I. (2019) "The least secure places in the universe? A systematic literature review on information security management in higher education", *Computers & Security,* 86, 350-357.

Bontis, N. (1998) "Intellectual capital: an exploratory study that develops measures and models", *Management Decision,* 36(2), 63-76.

Borgman, C. L. (2018) "Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier", *Berkeley Technology Law Journal,* 33(2), 365.

Bryman, A. and Bell, E. (2015) *Business research methods,* Fourth ed.*,* Oxford: Oxford University Press.

Chapman, J. (2019) "How safe is your data? Cyber-security in higher education", *HEPI Policy Note*, 12, 1-6, available: https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf [accessed 30 April 2019].

Christopher, J. (2014) "Australian public universities: are they practising a corporate approach to governance?", *Studies In Higher Education,* 39(4), 560-573.

Collini, S. (2017) *Speaking of universities,* London: Verso.

Corbin, J. M. and Strauss, A. L. (2015) *Basics of qualitative research: techniques and procedures for developing grounded theory,* Fourth ed.*,* Los Angeles: SAGE.

De Mauro, A., Greco, M. and Grimaldi, M. (2016) "A formal definition of Big Data based on its essential features", *Library Review,* 65(3), 122-135.

Desouza, K. C. (2006) "Knowledge Security: An Interesting Research Space", *Journal of Information Science and Technology,* 3(1), 1-7.

Desouza, K. C. and Vanapalli, G. K. (2005) "Securing knowledge in organizations: lessons from the defense and intelligence sectors", *International Journal Of Information Management,* 25(1), 85-98.

Di Berardino, D. and Corsi, C. (2018) "A quality evaluation approach to disclosing third mission activities and intellectual capital in Italian universities", *Journal of Intellectual Capital,* 19(1), 178-201.

Dierickx, I. and Cool, K. (1989) "Asset stock accumulation and sustainability of competitive advantage", *Management science,* 35(12), 1504-1511.

Doherty, N. F., Anastasakis, L. and Fulford, H. (2009) "The information security policy unpacked: A critical study of the content of university policies", *International Journal Of Information Management,* 29(6), 449-457.

Dretske, F. I. (1981) *Knowledge and the flow of information,* Oxford: Blackwell.

Edvinsson, L. and Sullivan, P. (1996) "Developing a model for managing intellectual capital", *European management journal,* 14(4), 356-364.

Elena-Pérez, S., Saritas, O., Pook, K. and Warden, C. (2011) "Ready for the future? Universities' capabilities to strategically manage their intellectual capital", *foresight,* 13(2), 31-48.

Etzkowitz, H., Webster, A., Gebhardt, C. and Terra, B. R. C. (2000) "The future of the university and the university of the future: evolution of ivory tower to entrepreneurial paradigm", *Research Policy,* 29(2), 313-330.

Field, M. (2019) "Oxford University 'right to be concerned' over China trade secrets theft, MP warns", *The Telegraph*, available: https://www.telegraph.co.uk/technology/2019/01/18/oxford-university-right-concerned-china-trade-secrets-theft/ [accessed 1 November 2019].

Gallardo Echenique, E., Marqués Molías, L. and Bullen, M. (2015) "Students in higher education: Social and academic uses of digital technology", *International Journal of Educational Technology in Higher Education,* 12(1), 25-37.

Hina, S. and Dominic, D. D. (2016) "Information security policies: Investigation of compliance in universities", in IEEE, ed. *3rd International Conference on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, Malaysia, 15-17 August 2016, IEEE, 564-569.

Hudson, W. J. (1993) *Intellectual capital: How to build it, enhance it, use it,* New York: Wiley.

Jupp, V. (2006) *The SAGE dictionary of social research methods,* Thousand Oaks, CA: SAGE Publications.

Kumar, N., Stern, L. W. and Anderson, J. C. (1993) "Conducting Interorganizational Research Using Key Informants", *The Academy of Management Journal,* 36(6), 1633-1651.

La Torre, M., Dumay, J. and Rea, M. A. (2018) "Breaching intellectual capital: critical reflections on Big Data security", *Meditari Accountancy Research,* 26(3), 463-482.

Lane, T. (2007) *Information security management in Australian Universities: An exploratory analysis*, Masters by Research, Brisbane, QLD: Queensland University of Technology.

Leal, C., Meirinhos, G., Loureiro, M. and Marques, C. (2017) "Cybersecurity Management, Intellectual Capital and Trust: A New Management Dilemma", in *9th European Conference on Intellectual Capital ECIC*, Lisbon, Portugal, 6-7 April 2017, 171-181.

Leitner, K.-H., Elena-Pérez, S., Fazlagić, J., Kalemis, K., Martinaitis, Ž., Secundo, G., Sicilia, M.-A. and Zaksa, K. (2014) *A Strategic Approach for Intellectual Capital Management in European Universities. Guidelines for Implementation*, Bucharest, Romania.

Liu, C.-W., Huang, P. and Lucas, H. (2017) "IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the US Higher Education", in eLibrary, A., ed. *International Conference on Information Systems ICIS 2017*, Seoul, South Korea, 10-13 December 2017, AIS Electronic Library,

Low, M., Samkin, G. and Li, Y. (2015) "Voluntary reporting of intellectual capital", *Journal of Intellectual Capital,* 16(4), 779-808.

Luker, M. A. and Petersen, R. J. (2003) *Computer and network security in higher education,* San Francisco, CA: Jossey-Bass.

Mariani, G., Carlesi, A. and Scarfò, A. A. (2018) "Academic spinoffs as a value driver for intellectual capital: the case of the University of Pisa", *Journal of Intellectual Capital,* 19(1), 202-226.

Marshall, C. and Rossman, G. B. (2011) *Designing qualitative research,* 5th ed., Thousand Oaks, CA: Sage Publications.

Martin-Sardesai, A. and Guthrie, J. (2018) "Human capital loss in an academic performance measurement system", *Journal of Intellectual Capital,* 19(1), 53-70.

McGowan, M. (2019) "China behind massive Australian National University hack, intelligence officials say", *The Guardian,* 6 June 2019,

Mejia, W. (2016) "Case Study: Time Line of DDoS campaigns against MIT", *Akamai's state of the internet security*, 1-10, available: https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/timeline-of-ddos-campaigns-against-mit-threat-advisory.pdf [accessed 12 March 2018].

Meritum Project (2002) *Guidelines for managing and reporting on intangibles (Intellectual capital report)*, Madrid, Spain: Fundación Airtel-Vodafone.

Miles, M. B. and Huberman, A. M. (1984) "Drawing Valid Meaning from Qualitative Data: Toward a Shared Craft", *Educational Researcher,* 13(5), 20-30.

Mouritsen, J., Johansen, M. R., Larsen, H. and Bukh, P. (2001) "Reading an intellectual capital statement: describing and prescribing knowledge management strategies", *Journal of Intellectual Capital,* 2(4), 359-383.

Moustaghfir, K. and Schiuma, G. (2013) "Knowledge, learning, and innovation: research and perspectives", *Journal of knowledge management,* 17(4), 495-510.

Nahapiet, J. and Ghoshal, S. (1998) "Social capital, intellectual capital, and the organizational advantage", *Academy of Management Review,* 23(2), 242-266.

Nambisan, S. (2017) "Digital Entrepreneurship: Toward a Digital Technology Perspective of Entrepreneurship", *Entrepreneurship Theory and Practice,* 41(6), 1029-1055.

Nambisan, S., Lyytinen, K., Majchrzak, A. and Song, M. (2017) "Digital Innovation Management: Reinventing Innovation Management Research In A Digital World", *MIS Quarterly,* 41(1), 223-238.

Paloma Sánchez, M. and Elena, S. (2006) "Intellectual capital in universities: Improving transparency and internal management", *Journal of Intellectual Capital,* 7(4), 529-548.

Paloma Sánchez, M., Elena, S. and Castrillo, R. (2009) "Intellectual capital dynamics in universities: a reporting model", *Journal of Intellectual Capital,* 10(2), 307-324.

Paoloni, P., Cesaroni, F. M. and Demartini, P. (2019) "Relational capital and knowledge transfer in universities", *Business Process Management Journal,* 25(1), 185-201.

Patton, M. Q. (2002) *Qualitative research and evaluation methods,* 3rd ed., Thousand Oaks, CA: Sage Publications.

Quinn, J. B. (1992) *Intelligent Enterprise: A Knowledge and Service Based Paradigm for Industry,* New York, NY: The Free Press - Simon and Schuster.

Ramírez, Y., Lorduy, C. and Rojas, J. A. (2007) "Intellectual capital management in Spanish universities", *Journal of Intellectual Capital,* 8(4), 732-748.

Ramirez, Y., Tejada, A. and Manzaneque, M. (2016) "The value of disclosing intellectual capital in Spanish universities A new challenge of our days", *JOURNAL OF ORGANIZATIONAL CHANGE MANAGEMENT,* 29(2), 176-198.

Rapetti, E. and Cantoni, L. (2010) ""“Digital Natives” and learning with the ICTs. The “GenY @ work” research in Ticino, Switzerland", *Je-LKS : Journal of e-Learning and Knowledge Society,* 6(1).

Renaud, K., Von Solms, B. and Von Solms, R. (2019) "How does intellectual capital align with cyber security?", *Journal of Intellectual Capital,* 20(5), 621-641.

Sangiorgi, D. and Siboni, B. (2017) "The disclosure of intellectual capital in Italian universities What has been done and what should be done", *Journal of Intellectual Capital,* 18(2), 354-372.

Schultze, U. and Leidner, D. E. (2002) "Studying knowledge management in information systems research: discourses and theoretical assumptions", *MIS Quarterly*, 213-242.

Secundo, G., Dumay, J., Schiuma, G. and Passiante, G. (2016) "Managing intellectual capital through a collective intelligence approach: an integrated framework for universities", *Journal of Intellectual Capital,* 17(2), 298-319.

Secundo, G., Elena-Perez, S., Martinaitis, Ž. and Leitner, K.-H. (2015) "An intellectual capital maturity model (ICMM) to improve strategic management in European universities: A dynamic approach", *Journal of Intellectual Capital,* 16(2), 419-442.

Secundo, G., Massaro, M., Dumay, J. and Bagnoli, C. (2018) "Intellectual capital management in the fourth stage of IC research: A critical case study in university settings", *Journal of Intellectual Capital,* 19(1), 157-177.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014) "Employees’ adherence to information security policies: An exploratory field study", *Information & Management,* 51(2), 217-224.

Soomro, Z., Shah, M. and Ahmed, J. (2016) "Information security management needs more holistic approach: A literature review", *International Journal Of Information Management,* 36(2), 215-225.

Spiggle, S. (1994) "Analysis and Interpretation of Qualitative Data in Consumer Research", *Journal of Consumer Research,* 21(3), 491-503.

Stenmark, D. (2000) "Leveraging Tacit Organizational Knowledge", *Journal of Management Information Systems,* 17(3), 9-24.

Stewart, T. A. (1997) *Intellectual Capital: The New Wealth of Organizations,* 2nd ed.*,* New York, NY: Nicholas Brealey Publishing.

Tien, J. M. (2013) "Big data: Unleashing information", *Journal of Systems Science and Systems Engineering,* 22(2), 127-151.

Timmermans, S. and Tavory, I. (2012) "Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis", *Sociological Theory,* 30(3), 167-186.

Trkman, P. and Desouza, K. C. (2012) "Knowledge risks in organizational networks: An exploratory framework", *The Journal of Strategic Information Systems,* 21(1), 1-17.

Tuomi, I. (1999) "Data is more than knowledge: Implications of the reversed knowledge hierarchy for knowledge management and organizational memory", in IEEE, ed. *32nd Annual Hawaii International Conference on Systems Sciences*, Maui, HI, 5-8 January 1999, IEEE, 1-12.

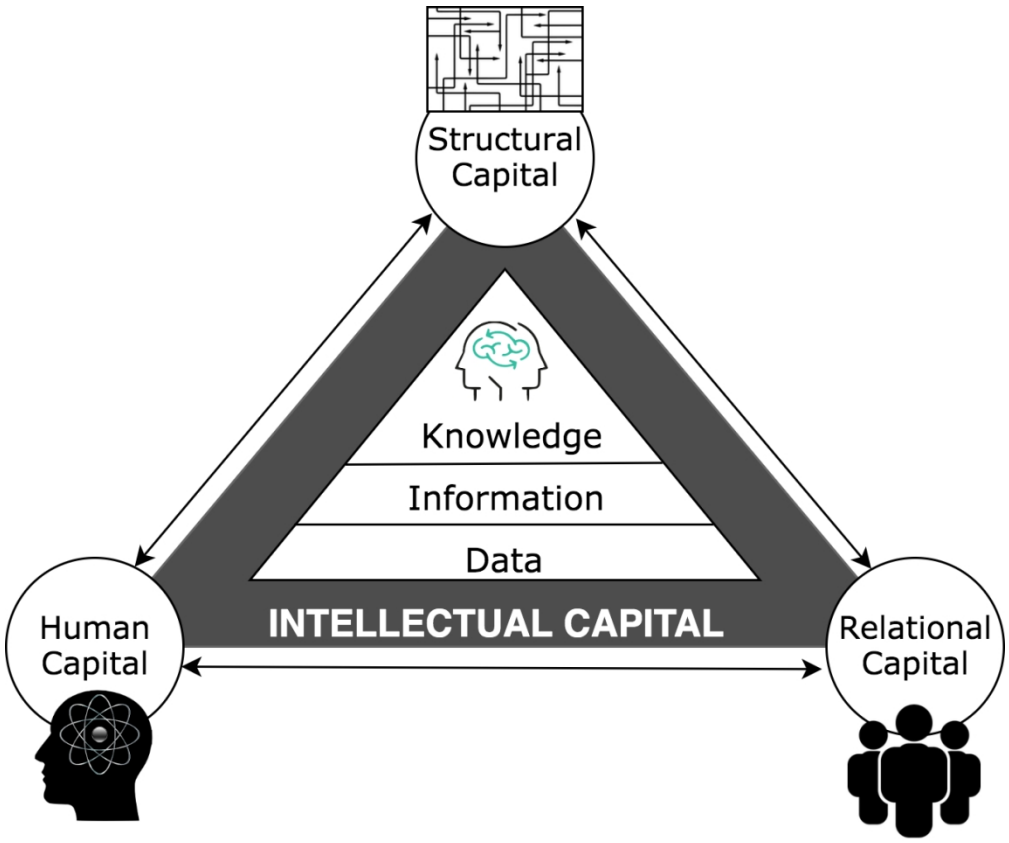
Vagnoni, E. and Oppi, C. (2015) "Investigating factors of intellectual capital to enhance achievement of strategic goals in a university hospital setting", *Journal of Intellectual Capital,* 16(2), 331-363.

von Solms, B. and von Solms, R. (2004) "The 10 deadly sins of information security management", *Computers & Security,* 23(5), 371-376.

Von Solms, B. and Von Solms, R. (2018) "Cybersecurity and information security–what goes where?", *Information & Computer Security,* 26(1), 2-9.

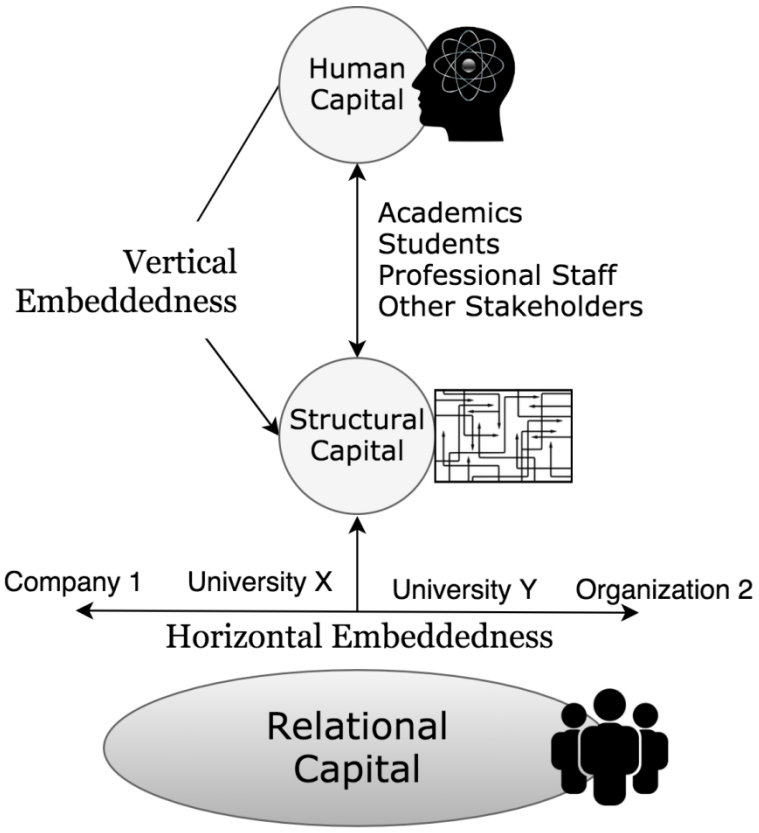
Von Solms, R. and Van Niekerk, J. (2013) "From information security to cyber security", *Computers & Security,* 38, 97-102.

Yeung, P. and Bennett, R. (2017) "University secrets are stolen by cybergangs", *The Times* [online], available: https://www.thetimes.co.uk/article/university-secrets-are-stolen-by-cybergangs-oxford-warwick-and-university-college-london-r0zsmf56z [accessed 1 March 2018].



Conceptual Framework

477x397mm (72 x 72 DPI)



Vertical and horizontal embeddedness in universities and relationships with IC components

542x446mm (72 x 72 DPI)

Table I: Ramirez, Tejada, and Manzaneque's definitions of IC components in universities, expanded with other sources for further details (indicated) (2016)

Component of IC	*Definition (and sources)*	*Examples in universities*
Human Capital	Explicit and tacit knowledge of university staff. Knowledge that employees take with them when they leave the firm: individuals' genetic inheritance, education, experience, attitudes, knowledge, abilities, skills, and motivation (Meritum Project, 2002; Hudson, 1993).	Academics, students, PhD students, professional staff, research fellows, career pathways.
Structural Capital (Organizational and Technological capital)	Explicit knowledge relating to processes of dissemination, communication and management of knowledge. Divided in: - Organizational capital: operational university environment, with its research activities, management, processes, corporate culture, organizational routines, etc. - Technological capital: technological resources including databases, licenses, software, archives, etc.	Research outputs (publications and patents); knowledge creation processes and projects (seminars and research projects); impact and artefacts of scientific research (best practices, integrated research centers, guidelines and protocols, records, databases); outputs of teaching (training); educational outputs.

Relational Capital	Economic, political and institutional relations with external stakeholders. Resources related to external relations with consumers, users, partners, and stakeholders; value of a company's franchise (Stewart, 1997; Mouritsen *et al.*, 2001).	Relations with regional, national and international commissions; associations and scientific societies; spin-offs; non-affiliated academics in universities; social context and volunteering sector.

Table II: A synthesis of data, information and knowledge security issues emerging from the research, as themes emerging from the data (regular font), interviews' excerpts (italics) or hypothetical, real-world examples not directly discussed in the interviews (in [ ] brackets).

	Data Security	*Information Security*	*Knowledge Security*
Human Capital		Spear phishing and social engineering	[despite hard to configure, this instance could be the case in which a criminal organisation 'poaches' a researcher away from a university after discovering their unique knowledge through illicit means]
	End-point vulnerability		
	Data and information security not always perceived as core business		
	Insider threats (malicious and unintentional)		
	IoT and BYOD misuse		
	"…we manage over 100,000 identities"		
Structural Capital			
Organisational	*"The consequences of not following good cyber-security practices are probably not well understood."*		
	Organisational policies and practices in data and information security		
			Reputational aspects associated with knowledge protection, as

	Data Security	*Information Security*	*Knowledge Security*
			discussed in board meetings
			"As an IT manager, how do you communicate with company directors in non-technical ways, as they usually do not come from an IT background?"
	"Maybe in two years' time someone may be: 'Well, security had enough money in the last years, now it's time to invest in something else.'"		
Technological	*"The only thing that will give you absolute security … is disconnecting from the Internet and you put your technology in Fort Knox"*		[an attacker exploits a vulnerability in an interactive educational platform to appropriate teaching materials about a piece of technology under development, with significant commercial potential]
	Some software patching could compromise researchers' working environment		
	Universities' increasing attack surface		

	Data Security	*Information Security*	*Knowledge Security*
	Structural weaknesses of security architectures		
	DDoS attacks		
	Contagion effects caused by the presence of green-field and legacy systems simultaneously		
Relational Capital		Insider threats guided by external agents to capture knowledge and IP	
	Longer supply chains and complex outsourcing arrangements		
	External media reports on eminent cyber-breaches		
	"Anyone can be a hacker. Kids coming out of school have much more IT knowledge than people that just graduated a couple of years ago."		

Interview schema:

After reading the *participant information sheet* and signing the *consent form* to agree to voluntarily participate in the semi-structured interview and having the interview recorded by the researcher, participants were asked several prompting questions. Given the semi-structured interviews format, participants were allowed to elaborate on their answers beyond a strict reply to the question. Based on this, the researchers could ask follow-up questions on a case-by-case basis, which are not included among the following prompting questions:

- *What are the current and future cyber-threats that your organisation is facing and will likely face in the future?*
- *What do you think are the critical data and information security risks for your organization?*
- *What factors, in the present, lead you to believe that each of these is critical?*
- *How do data and information security risks currently inform strategic decision-making in your organization? Why?*
- *Do you think information security is a human or a technical issue? Why?*

- *What do you think will be the impact of the Notifiable Data Breaches scheme[1]?*
- *If you had the 'magic wand', what would you do to help your organisation with managing its information securely?*

[1] The Australian legislation that mandates public disclosure of data breaches by public and private organisations, entered into force in February 2017.